Bird & Bird

European Data Protection Monthly Bulletin

December 2022

Welcome to our regular European Data Protection Bulletin

In this edition, we bring you the following updates:

EDPB

Date	Description
10 October	**Opinion 28/2022 on the Europrivacy Certification** On 10 October 2022, the EDPB adopted its Opinion on the Europrivacy criteria of certification, approving its certification mechanism as a data protection seal under GDPR Article 42(5). **Background** Article 42 (1) GDPR requires the EDPB and European Commission to encourage the establishment of data protection certification mechanisms and of data protection seals and marks (collectively referred to as 'certification mechanisms'). The purpose is to provide a method for controllers and processors to demonstrate compliance with the GDPR and enhance transparency. It can also help individuals assess the level of data protection for a particular product or service. EU-wide certification mechanisms must undergo an extensive approval process, with the EDPB Opinion describing aspects of this approval process for the Europrivacy certification mechanism. This mechanism is a criteria of certification drafted by the European Centre for Certification and Privacy and submitted to the EDPB by the Supervisory Authority of Luxembourg. **Scope and Europrivacy certification requirements** The scope of the Europrivacy certification mechanism is defined during the application process. While the certification is a general scheme, in that it can be applied to any processing activity, certification is not intended to cover an organisation in a blanket fashion, and would instead only apply to a specific processing activity/ies (which would be defined during the application process). The Opinion approves the various criteria of the Europrivacy certification scheme, including requirements for applicants to: • identify the components of processing operations; • check the lawfulness of processing for each processing operation; • demonstrate compliance with the data protection principles; • evaluate processor-controller contractual agreements;

- implement measures relating to individual rights;
- assess the risk to the rights and freedoms of individuals;
- apply technical and organisational measures; and
- identify all personal data transfers to third countries and international organisations and ensuring that appropriate safeguards are in place

The Opinion concludes by approving the Europrivacy certification mechanism.

Practical considerations

The Europrivacy mechanism is the first certification mechanism approved by the EDPB. At a basic level, it provides an opportunity for organisations to demonstrate compliance with the GDPR and enhance transparency. Additionally, it can help individuals have confidence in the level of data protection at the organisation, adding value to the organisation and providing an incentive to good data protection practices.

The Europrivacy certification process is therefore rigorous, and has certain minimum requirements, such as the need to have a DPO and a ROPA (even if these are not legally required by the GDPR). Certification is not permanent, and is subject to a regular renewal process.

Europrivacy certification will not have any impact on liability (i.e., it would not mean that an organisation receives more favourable enforcement action), but it can be used to demonstrate compliance in such an event.

A link to the Opinion can be found here and further details on the Europrivacy certification mechanism can be found here.

18 October

Updated Guidelines on Personal Data Breach Notification - More Stringent Rules for Non-EEA companies

In October, the EDPB opened a public consultation (now closed) on a specific section (para 73) of its Guidelines on Personal Data Breach Notification creating more onerous data breach reporting requirements for businesses based entirely outside the EEA.

Previously when companies based entirely outside the EEA were required to notify a supervisory authority of a data breach, the recommendation was that they only needed to notify the supervisory authority of their GDPR Representative's country. This originated in the WP29 guidelines on personal data breach notification (WP250) and had persisted in the original EDPB guidelines.

Instead, the EDPB confirms that the mere presence of a representative does not trigger the one stop shop system and is now directing these companies to report the breach to all the supervisory authorities where affected data subjects reside. This is a much more onerous requirement, as this could easily result in needing to make up to 27 reports all within the tight 48-hour turnaround for such reports.

While the data breach reporting forms are becoming increasingly standardised, it would still be useful to find ways to minimise the impact of this change. The main route will be for affected companies to ensure their ROPAs are up to date and the relevant member states for each processing activity

are identified. This will allow for a quick determination of who the company will need to report to, in the event that a reportable breach occurs, and avoid both the risk of under-reporting and the expense of over-reporting.

A link to the Guidelines can be found here.

21 October

Guidelines identifying a controller or processor's lead supervisory authority

On 21st October 2022, the EDPB opened a public consultation on specific sections of its guidelines on identifying a controller or processor's lead supervisory authority. The sections subject to consultation relate to the designation of a lead supervisory authority in joint controllership situations. At the outset, the EDPB restates the position adopted in its 2020 guidelines on the concept of controller and processor, namely that joint controllers must determine "who does what" by deciding between themselves who will carry out which tasks in order to ensure that their processing complies with the GDPR. According to the EDPB, this responsibility extends to the organisation of contact with data subjects and supervisory authorities.

The EDPB places limits on joint controllers' capacity to determine their own arrangements, however, highlighting that supervisory authorities are not bound by the terms of joint controller arrangements, neither on the issue of the qualification of the parties as joint controllers nor on their designated contact point. Accordingly, the decision-making power of joint controllers does not extend to the determination of the competent supervisory authority, or the ability of these supervisory authorities to exercise their powers in accordance with Articles 57 and 58 of the GDPR. To this end, the EDPB states that the concept of a 'main establishment' cannot extend to joint controllership situations and that as a result, joint controllers cannot designate a common main establishment for both controllers.

The guidelines set out the following roadmap, to be used by joint controllers in determining the appropriate lead supervisory authority:

i. Check if the joint controllers are established in the EEA;
ii. Identify the place of central administration in the EEA for each joint controller respectively (where applicable);
iii. The supervisory authority of the country where the place of central administration is located is the lead supervisory authority of the respective joint controller.

The public consultation closed on 2nd of December. A link to the Guidelines, which are still in draft form, can be found here.

17 November

Latest Updates to EU BCRs – what you need to know

On 17 November, the EPDB published its long awaited draft Recommendations to update the Controller Binding Corporate rules Application Form and Requirements table (now called "Elements and Principles to be found in BCR-C") which are open to consultation until 10 January 2023. These will affect all organisations holding existing EU Controller BCRs as well as those currently going through the application process or thinking of doing so. Whilst the main driver behind the update is to build in requirements to address Schrems II (i.e. to deal with transfer impact assessments and Government access

requests), the EDPB has also taken the opportunity to build on and revise other requirements. These Recommendations are intended to replace and repeal the former Article 29 Working Party documents: WP 264 and WP 256 rev.01.

In order to help affected organisations quickly assess the scope of the changes to the Requirements table, we have produced the following two documents:

(i) Aa simple track changes version of the Requirements showing all the changes between the new Requirements and those originally set out in WP 256 rev.01 (marked as version 1); and

(ii) an "edited" track changes version of the Requirements where minor changes and/or sections which have just been moved around the document are not highlighted, leaving track changes which are more significant in nature and/or which are likely to require organisations to carefully check their existing or draft EU Controller BCRs to see if further amendments are likely to be needed (marked as version 2).

Please click here to download both documents and see a short summary of the changes.

A link to the Recommendations can be found here

CJEU

Date	Description
6 October	**CJEU Advocate General's opinion on GDPR damages: No punitive damages – no damages without proof – no "de-minimis" damages (Case C-300/21. UI. v. Österreichische Post AG).** In an opinion delivered on 6 October, the Advocate General of the European Court of Justice ("AG") delivered his long-awaited view on fundamental questions regarding non-material damages under Art. 82 GDPR. The AG provided a rather balanced interpretation and amongst other things considered that mere "annoyance" about a breach of duty by the controller is not compensable. Also, mere loss of control over data as such does not necessarily justify a claim for damages. If the CJEU decides to follow the AG's opinion, proving damage under the GDPR will become more challenging for data subjects. **Background** The case was referred to the CJEU by the Supreme Court of Austria. This case involved the Austrian Postal Service (Österreichische Post AG) which had collected the personal data of millions of Austrians and used an algorithm to make a statistical projection to link individuals with a potential political party affinity in order to sell this result for election advertising. An individual who did not consent to such processing of his data and who had learned via an access request that he supposedly had a high affinity with a right wing group, filed a lawsuit, seeking a compensation payment of EUR 1,000 for non material damages claiming that he was upset, angered and offended by this wrongful political affiliation, stating that it was insulting and shameful as well as extremely damaging to his reputation. The first instance and second instance courts dismissed the damages claims but the Austrian Supreme Court referred the following questions to the CJEU for a preliminary ruling (Article 267 Treaty on the Functioning of the EU): a) Is an infringement of the GDPR sufficient to justify a claim for damages under Art. 82 GDPR, or is proof of suffered harm required in addition? b) What are the requirements under EU law for the assessment of damages? c) Does a certain threshold have to be exceeded for the assumption of non-material damage, or is the upset caused by the infringement already sufficient as damage?

No compensation without proof of damage

According to the AG, presentation and proof of a specific damage is a prerequisite for an Art. 82 GDPR claim. The AG refers to the wording of Art. 82 GDPR ("damages suffered") and Recital 146 sentence 6 (which mentions damage "suffered"). According to the AG, the GDPR does not provide for an irrebuttable presumption that an infringement of the GDPR automatically constitutes a damage to data subjects. Rather, whether or not the GDPR infringement results in damage for the data subject remains to be established in each individual case.

GDPR does not provide for "punitive damages"

The AG clarified that the GDPR does not provide for a system of punitive damages.The AG saw the aim of Art. 82 GDPR as primarily to compensate the injured data subject, rather than sanctioning or deterring. For the calculation of a compensation claim, this means that the amount must reflect the actual damage suffered but cannot go beyond.

Loss of control over data is not per se a damage

The AG concluded that the GDPR does not grant data subjects control over personal data as a right in itself. Loss of control over data is therefore not necessarily compensable damage within the meaning of Art. 82(1) GDPR.

A "de minimis threshold" must be exceeded

The AG confirmed that a damage under Article 82 para. 1 GDPR requires that a certain materiality threshold is exceeded. The AG left it to the courts of the Member States to differentiate between mere inconveniences due to a GDPR infringement and actual damages. The AG concluded that any breach of the GDPR may lead to a certain level of "annoyance or upset", but not every infringement can automatically lead to a damage. Data subjects should first resort to other remedies provided by the GDPR (e.g. a complaint under Art. 77 GDPR).

Outlook

The CJEU is not bound by, yet often follows the AG's preparatory opinions. If the CJEU agrees with the AG (and a decision is expected for February/March 2023), data controllers can more comfortably defend themselves against damage claims from data subjects in the future. It remains to be seen, however, how national courts of the Member States will interpret materiality thresholds for a damage and how they differentiate between "mere inconveniences due to a GDPR infringement" and "actual damages".

Information Commissioner's Office (ICO)

Date	Description
September	**Updated Guidance on Governance of CCTV, Video Surveillance post deployment** The ICO has updated its existing video surveillance guidance. This guidance provides advice for organisations who operate video surveillance systems that view or record individuals. It also covers information that relates to individuals, for example vehicle registrations captured by Automatic Number Plate Recognition (ANPR) equipment as well as the use of Facial Recognition Technology (FRT) and machine learning algorithms. The guidance covers how to demonstrate accountability and how to carry out a DPIA for using FRT In particular, updates have been made to the chapter on Governance of CCTV, Video Surveillance post deployment which deals with: -how to disclose surveillance footage to third parties; -how to comply with rights of individuals and making sure staff know how to recognise such requests and deal with them efficiently; -how to redact information relating to third parties. For example, using techniques such as blurring, masking, or using a solid fill to completely obscure parts of the footage; and -requests for surveillance footage made to public authorities under the Freedom of Information Act 2000 for information captured by surveillance systems.
October	**Employment practices: Monitoring at Work and Information about Worker's Health Guidance** The ICO is currently producing specific guidance on employment practices and data protection. On 12th October, the ICO released its draft guidance on Monitoring at Work. This guidance is open for consultation until 11 January 2023.

	The draft guidance aims to provide practical tips about how best to monitor workers in accordance with data protection legislation and best practice. This includes information about how and when you can monitor employees. This includes automated processes such as monitoring tools, human oversight and whether you must let your employee know. The draft guidance covers systematic monitoring, where an employer monitors all workers or groups of workers as a matter of course such as using software to monitor productivity but it also applies to occasional monitoring, where an employer introduces monitoring as a short-term response to a specific need. This includes installing a camera to detect suspected theft. On 27th October, the ICO released its draft guidance on Information about Worker's Health. This guidance is open for consultation until 26 January 2023. The draft guidance covers lawful bases for processing health information relating to workers, handling sickness and injury records, occupational health schemes, medical examinations, testing and monitoring, genetic testing and sharing health information with others.
October	**Two New Research Reports published on Biometrics technologies** The ICO has published two new reports to help support businesses who are using new emerging biometrics technologies: Biometrics: Insight and Biometrics: Foresight. The ICO has heavily emphasised why technologies should be curated with privacy and the protection of humans at the forefront from the outset and during the design. The Insight report sets out the grounds of the ICO's research, core definitions and technical and legal contexts that are used to understand the potential challenges that may emerge and the idea is to provide a short guide for those who wish to know more about the current state of biometric technologies from a regulatory perspective. The Foresight report then considers the privacy implications of these technologies in the near future, setting out some use case scenarios across different sectors (finance, entertainment, wellbeing, employment and education). These scenarios highlight key issues relating to the use of such technologies such as: • The need to clarify key terminology and definitions surrounding biometric technologies and data. • The increased use of biometric technologies for classification and where this sits under existing data protection legislation. • The need for compliance with transparency and lawfulness requirements when processing ambient data. • The need to understand and appropriately manage high risk biometric technologies, such as emotional AI. The ICO will be producing more detailed guidance on biometrics by Spring 2023 which will set out core definitions and approaches, link to existing ICO guidance, identify emergent risks and user based or sector specific case studies to highlight good practice.

For more information: https://ico.org.uk/about-the-ico/research-and-reports/biometrics-technologies/

November

How to use AI and Personal Data

On 11 November, the ICO published this document which it describes as top tips providing a brief introduction to some of the most important considerations organisations should make when using AI and personal data, and dealing with some FAQ identified by the ICO.

The guidance identifies the following key themes and steps:

- The use of AI will necessitate a DPIA and there will be a requirement to consult with the ICO where it is not possible to mitigate high risks. The guidance emphasizes the importance of consulting with affected groups when assessing the risks presented by the processing to ensure the impact of the processing on such groups is fully considered;
- The barriers to making the processing transparent including with respect to the context of processing, the expectations of the data subject, and how individual rights will be respected;
- The daunting nature of the principle of data minimization which can be particularly problematic in the context of training data. The ICO suggests synthetic data and federated learning as tools which should be considered to minimise the amount of personal data being processed;
- Addressing bias and discrimination. The ICO recommends ensuring data quality to reduce bias. Additionally, mapping out the likely effects of the system and assessing whether they will be acceptable;
- Preparing the data appropriately. The ICO suggests consulting with members of protected groups on appropriate ways to label the data, and emphasizes the importance of a rigorous approach to labelling.
- Ensuring security of the AI system. The Guidance recognises that appropriate measures will depend on the particular system, but suggests broadly applicable principles like debugging and monitoring for anomalies.
- The guide includes also includes a reminder of the prohibition on automated individual decision making with legal and similarly significant effects.
- The closing piece of advice relates to the use of a supplier's AI and highlights that where the organisation is acting as a controller, the obligations will apply in the same way regardless of who has supplied the AI

  The guidance document is quite short and high level, but it really serves to introduce key concepts in a layered approach with each section signposting more detailed guidance.

The full guidance and links are available here: https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf

November	**New guidance on ICO Audits and Artificial Intelligence Audits** The ICO recognises that its audit powers play a key role in educating and assisting organisations to meet their obligations and as such, the ICO carries out a programme or consensual and compulsory audits across private and public sector organisations to assess their processing of personal data and to provide practical advice and recommendations. Organisations can request these audits (which are free) but the ICO will take a risk-based approach in prioritising organisations. Given the fact that AI continues to permeate many aspects of our lives, the ICO has developed a new framework for auditing AI which allows companies to assess whether they are following good practice. The audit will focus on whether the organisation has implemented policies and procedures to demonstrate that it is acting in the best interests of an individual through the processing of personal data within the AI system and will assess whether the organisation has designed data protection safeguards into the development or deployment of these systems. The ICO will make recommendations to assist the organisations to mitigate the risks of non-compliance with UK data protection laws and following the audit, a report will be provided that gives an assurance rating for each scope area covered and highlighted the greatest risks and priorities to address. For more information: Audits | ICO
November	**ICO publishes new data transfer impact assessment tool and guidance** The ICO has published its new guidance on completing data transfer impact assessments, which it sets out as an alternative to the EDPB's approach. This is accompanied by a tool (a word based template) The ICO has emphasised that it is happy for controllers to take either approach, so companies who have already carried out a DTIA to the EDPB standard (or who need to meet the EDPB's standard due to direct application of the EU GDPR) there is no requirement to consider the ICO's alternative. However, its guidance and new tool may provide a simpler route for UK based organisations requiring less specific assessment of local legal remedies in recipient countries where the nature of the data being transferred is low risk. The ICO emphasises that it has aimed to find: "an alternative, achievable approach delivering the right protection for the people the data is about, whilst ensuring that the assessment is reasonable and proportionate." The key question for the ICO, according to their guidance, is: "whether, as a result of the transfer, there is any increase in the risk to people's privacy and other human rights, compared with the risk if the information remains in the UK.

The ICO's tool focusses on the inherent risk of a dataset in context. Three different levels of investigation, which are only triggered if data types of a moderate or high risk is to be transferred. Many types of data are considered low risk, including age, name, contact details, and employment details. More surprising and controversial is a statement that all free text should be considered high risk, because organisations "must assume is SCD".

For higher risk transfers, the ICO approach may not prove simpler that the EDPB route: the tool encourages consideration of human rights risks and the ability to enforce the transfer mechanism for these categories, and explains that professional advice might need to be sought to determine this. But for lower risk data transfers, this tool may offer a simpler route to completion of DPIAs for UK controllers.

For more information: International transfers | ICO

December

ICO publishes updated Detailed Guidance on Direct Marketing

The ICO has published its new detailed direct marketing guidance. This follows on from the ICO's publication, in January 2020, of its draft replacement for its statutory direct marketing code of practice. The ICO has not formally published this as a replacement of its statutory code, but it is expected that this guidance will be laid as the new code once any changes are made following the government's planned DP reforms.

Notably, this detailed guidance is much shorter that the draft code, coming in at 58 pages down from 124. Sections on profiling and online advertising have been removed, as have pointed suggestions that consent is likely needed for certain profiling activities falling outside of PECR consent obligations.

Remaining from the draft code are detailed explanations of what the ICO considers to be direct marketing – although again this takes a slightly less strident approach: an example statement that "Your local supermarket stocks carrots" is promotional in tone is replaced by the slightly clearer "Your local supermarket stocks leading brands". The detailed guidance also helpfully notes examples that might not be considered marketing messages, acknowledging that some reminders of customer benefits – if "factual" such as "reminding customers that their bank account includes free travel insurance" may not be considered marketing. Although promising, this remains a difficult line to tread in light of ICO's continued enforcement over service messages.

Other UK News

Date	Description
November	**Update on UK Data Reform** The Data Protection and Digital Information Bill was laid before Parliament on **18 July 2022** and was scheduled for its second reading on **5 September 2022**. The second reading was removed until further notice, following the election of Elizabeth Truss as new Conservative Party leader and the appointment of a new Secretary of State for Digital, Culture, Media and Sport, to allow ministers to consider the legislation further, see business statement issued on 5 September 2022. Reform of UK GDPR is still very likely, particularly as Michelle Donelan (Secretary of State for DCMS) announced in her speech on 3 October 2022 the intent to replace the GDPR with new legislation. While this speech seemed to indicate that there would be a further round of public consultation and that the Bill would be significantly amended, it is currently unclear the extent to which changes will be made. Owen Rowland, Deputy Director for Domestic Data Protection Policy, DCMS said at the IAPP conference in Brussels in November that the latest consultation on the Bill will commence shortly. The Bill currently proposes amendments to important areas such as: • Narrowing the definition of 'Personal Data'; • Reform of the accountability framework; • A risk-based approach to international transfers; • A list of recognised legitimate interests that would negate the need to carry out the balancing test (although not the necessity test); • Softening the requirements regarding automated decision making (where it does not involve special category data); and • Expanding the grounds for refusal in relation to subject access requests to cover vexatious or excessive requests.

UK ICO Enforcement

Date	Entity	Type of Breach & Sanction	Description of Breach
6 September	Halfords Limited	PECR Unsolicited direct marketing emails Monetary Penalty £30,000	The ICO has fined Halfords £30,000 for sending unsolicited marketing emails to individuals without their consent. This sanction highlights important lessons for organisations trying to argue that some of their communications are "service messages" rather than "direct marketing" messages. This issue came to the attention of the ICO following a complaint from an individual about an email that had been sent to them without consent. The email related to a 'Fix Your Bike' Government Voucher Scheme, which was a scheme run by the UK government, initiated on 28 July 2020, which allowed members of the public to receive a voucher worth up to £50 towards the cost of repairing a bicycle. The voucher could be used with bike repairers or mechanics that were registered for the scheme in England. 16. The email encouraged the recipient to book a free bike assessment and to redeem the voucher at their chosen Halfords store. The email did not contain an unsubscribe link. The email contained a disclaimer stating, "*This is a service message and does not affect your marketing opt-in* status", however, noting the promotional aspect of the email, the ICO was concerned that the email did appear to contain direct marketing material and was therefore subject to PECR. The ICO contacted Halfords to clarify why they thought that the contents of such an email would constitute "a service message" rather than direct marketing and to ask how many individuals who had not opted in to receive direct marketing had received a copy of the email. Halfords advised that they were relying on "legitimate interests" as the lawful basis for sending the email and that the email had been sent to 498,062 customers who had not

			previously opted into marketing (but all had bought a bike from Halfords in the last 3 years). In later correspondence, Halfords also tried to argue that this constituted a service message as it sought to inform customers that had previously purchased a cycle from Halfords of the new government voucher scheme, rather than promoting products and services at Halfords. However, Halfords did recognise that this could be interpreted as a marketing communication by customers. In further support of the claim that the email was a 'service' message, Halfords stated that: "*There are no links to the provision of Halfords services, sales or offers, only to the terms and conditions of voucher usage*", and "*The only messages in the campaign relate to how to obtain and redeem the voucher*". Halfords further denied a breach of PECR arguing that 3,700+ people took up the opportunity and claimed the voucher and there were only 7 complaints arising from almost half a million email service messages. They also argued that this was a one-off campaign to assist the government, and the UK, in its response to the pandemic in unique and unprecedented circumstances and that they had acted entirely in the public interest in its support of the government initiative and did not try and take advantage of this collaboration by promoting its own goods or services off the back of this service message. The ICO disagreed with the above views and found that the contents of the email were to be considered direct marketing (as they clearly advertised Halfords' services) and that therefore Halfords had acted in breach of PECR by sending such emails individuals without their consent. The ICO was also satisfied that the soft opt in exemption did not apply either, not least because the targeted recipients had already opted out of marketing (or rather had not opted in) and were in any event denied the opportunity of opting out at the point of receiving the email as it didn't contain a simple means of refusing the use of their contact details for direct marketing purposes.
26 September	TikTok	UK GDPR Failure to comply with children's privacy Notice of Intent to fine £27 million	The ICO has issued TikTok Inc and TikTok Information Technologies UK Limited with a notice of intent to fine them £27 million following an ICO investigation which found that they may have breached UK data protection law and failed to protect children's privacy when using the TikTok platform. In particular, the investigation provisionally found that TikTok may have:

			• processed the data of children under the age of 13 without appropriate parental consent, • failed to provide proper information to its users in a concise, transparent and easily understood way, and • processed special category data, without legal grounds to do so.
28 September	7 Companies	UK GDPR Non-Compliance with DSARs Reprimands	The ICO has taken action against seven organisations (including Virgin Media, MOD, Home Office and Kent Police) for failing to respond to data subject access requests (DSARs). This resulted in the issue of reprimands (under Art 58 UK GDPR) as well as (for the public authorities), practice recommendations under the Freedom of Information Act 2000. The issuing of reprimands against public authorities rather than monetary penalties is part of the ICO's revised approach to working more effectively with public authorities. The organisations were identified following complaints in relation to multiple failures to respond to DSARs either within the statutory timescales or at all. For example, Virgin Media had received over 9500 DSARs over a 6 month period in 2021 and 14% of these were not responded to during the statutory time period. The organisations have between 3 -6 months to make further improvements or further enforcement action could be taken.
5 October	Home Office	UK GDPR Reprimand	The ICO issued a reprimand to the Home Office after sensitive documents were found at public venue in London. The documents, which were handed by venue staff to police in September 2021, were classed as "Official Sensitive" and included two Extremism Analysis Unit Home Office reports and a Counter Terrorism Policing report and the reports also contained personal data relating to Police staff. The ICO found that the Home Office had failed to ensure an appropriate level of security for such persona data. The investigation also found that the Home Office did not have a specific sign-out process for the removal of documents from the premises, and the incident was not reported to the ICO within the 72 hour time limit.
6 October	Easy Life Limited	UK GDPR	The ICO has fined Easylife Limited: (i) £1,350,000 for using personal information of their customer to predict their medical condition and target them with health related products

		Breach of Art 5(1)(a) PECR Unsolicited direct marketing calls Enforcement Notice Monetary Penalty Notice of £1.48 million	without their consent in breach of the UK GDPR; (ii) £130,000 for making 1.3million predatory direct marketing calls. The ICO also issued an enforcement notice under PECR requiring Easylife to stop calling individuals who had opted out of direct marketing calls or who had registered with the TPS and who had not notified Easylife that they did not object to such calls being made. Easylife is a catalogue retailer that sells household items, as well as services and products under their Health, Motor, Supercard, and Gardening Clubs. The ICO discovered during its investigation that that when a customer purchased a product from Easylife's Health Club catalogue, the company would make assumptions about their medical condition and then market health-related products to them without their consent. The ICO also found that significant profiling of customers and 'invisible' processing of health data took place. Interestingly the ICO also quoted the recent CJEU case of OT v Vyriausioji tarnybines etikos komisija (Case C-184/20, 1 August 2022) which confirmed that the protections which the GDPR gives to data subjects' special category data, including health data, extend beyond inherently sensitive data to cover data revealing health data indirectly, following an intellectual operation involving deduction and cross-referencing. In a separate investigation the ICO found that, between 1 August 2019 and 19 August 2020, Easylife made 1,345,732 unwanted marketing calls to people registered with the Telephone Preference Service (TPS) in contravention of PECR (which states that live marketing calls should not be made to anyone who has registered with the TPS unless they have told the caller that they wish to receive calls from them.
19 October	Apex Assure Limited	PECR Unsolicited direct marketing calls to individuals registered on the TPS Enforcement Notice Monetary Penalty of £230,000	The ICO has fined Apex Assure Limited £230,000 (and issued an enforcement notice) for making 122 unsolicited direct marketing calls to subscribers who had listed their numbers on the TPS. This follows a number of other monetary penalties and enforcement notices issued against similar organisations earlier in the month for the similar breaches (eg GreenLogic Uk Limited, Eco Spray Insulations Limited, Euroseal Windows Limited and Post Windows UK Limited).

24 October	Interserve Group Limited	UK GDPR Monetary penalty of £4.4 million Breach of Article 5(1)(f) and Article 32 UK GDPR.	The ICO has fined Interserve Group Limited, a construction company. £4.4 million for failing to keep personal information of its staff secure. This fine provides a stark reminder for organisations the importance of keeping on top of software updates and training and that there is no room for complacency. The ICO found that Interserve failed to put appropriate security measures in place to prevent a cyber attack, which enabled hackers to access the personal data of up to 113,000 employees through a phishing email. The data included personal information such as contact details, national insurance numbers, and bank account details, as well as special category data including ethnic origin, religion, details of any disabilities, sexual orientation, and health information. The ICO commissioner stated "If your business doesn't regularly monitor for suspicious activity in its systems and fails to act on warnings or doesn't update software and fails to provide training to staff, you can expect a similar fine from my office." John Edwards
3 November	Cabinet Office	UK GDPR Reduction in Monetary Penalty	The ICO has agreed to reduce the £500,000 Monetary Penalty Notice (MPN) imposed on the Cabinet Office in 2021 in relation to the New Years Honours breach of £50,000 . This penalty was originally issued in November 2021 following an investigation into a data breach in 2019 where the Cabinet Office published a file on GOV.UK containing the names and unredacted addresses of more than 1,000 people announced in the New Year Honours list. The personal data was available online for a period of two hours and 21 minutes and it was accessed 3,872 times.
11 November	Zuwyco Limited	Monetary Penalties of £128,000 Enforcement Notice PECR 21(1)b)	Over the course of seven months, Zuwyco Limited made 93,558 unsolicited direct marketing telephone calls to people registered with the Telephone Preference Service (TPS), contrary to regulation 21(1)(b) of PECR. It is against the law to make a live marketing call to anyone registered with the TPS, unless they have told the organisation that they do not object to receiving calls from them. These calls resulted in 7 complaints being made to the TPS and the ICO. The ICO was also satisfied that the subscribers had registered with the TPS at least 28 days prior to receiving the calls and had not notified Zuwyco that they did not object to receiving such calls.

7 December	Allapplianceservices UK Limited Boiler Cover Breakdown Limited Boiler Breakdown Limited Repairs UK Limited Utility Guard Limited	Monetary Penalties of £435,000 Enforcement notice PECR	The ICO has fined five companies a total of £435,000 for collectively making nearly half a million unlawful marketing calls to people registered with the TPS. Some of the calls (which were trying to convince people to sign up for white goods insurance) were targeted directly at elderly vulnerable people. There was also evidence that pressure tactics were used with a view to obtaining payment details from the individuals called.

Date	Appellant	Type of Case and Result	Summary of Case
3 November	SR WIELEMAN	Handling of an ICO Complaint	An application to the Information Tribunal on the handling of the Applicant's complaint to the ICO was dismissed. The Applicant had complained to the ICO that a company by the name of Contactout had not responded to his DSAR. Contactout is a data controller based in the USA, thus classified as a 'third country' category of data controllers. The ICO argued that although it was able to communicate with the data controller regarding infringement of the data protection rights, any enforcement falls outside its powers and therefore it is unable to impose any actions to improve data protection practices within the organisation. Contactout's data policy specifies the ICO as being a supervisory authority. Nothing in the legislative scheme permits Contactout to confer jurisdiction on the ICO by naming the ICO in its documentation. Here the Applicant was based in the Netherlands, with no connection to the UK or Contactout. The Applicant claimed that no adequate explanation had been given as to why the ICO was not the supervisory authority. Whilst the court found that there was potential to fall within section 166 Data Protection Act 2018, here the appropriate steps had been taken, as there was no connection with the UK, so no enforcement powers were available. The application was dismissed on the basis of there being nothing left for the Commissioner to do that could form the basis for an order under s.166. A copy of the case can be found here: **S R Wieleman v Information ICO [EA/2022/0034/GDPR]**
7 November	Seaview Brokers Limited	Unsuccessful Challenge to PECR Monetary Penalty of £15,000 and Enforcement Notice	Seaview Brokers Ltd ("Appellant") unsuccessfully challenged two notices served by the ICO ("Respondent") for using a public telecoms service for the purpose of making unsolicited direct marketing calls, in violation of PECR. The Appellant purchased a direct debit book from the company 'Service Monkey', containing data supplied by

two third parties. The data had originally been obtained via a lifestyle survey which asked individuals to agree to telephone marketing from industry sectors listed at the end of the call; individuals were not able to finetune their preferences or 'opt out'. The Appellant gave each customer a new contract which included the right to be contacted by the Appellant. The ICO's investigation demonstrated the Appellant made repeated calls to the same individuals during June 2020. Around 400 individuals were called at least four times, with one number receiving 32 calls. The ICO searched complaints to the TPS and found a higher weekly incidence of calls to TPS numbers. The Appellant's proposition that the calls were 'welcome calls' was found by the court to be implausible due to the time and resources devoted in making the calls to customers who had been on the books for months. The Appellant had already introduced themselves in writing to the newly acquired customers. The court disregarded the lack of a relevant complaint, pointing out PECR's role as protective legislation whilst noting that people do not often complain, particularly vulnerable persons. The aggravating factors were upheld; the nature of services marketed (insurance of white goods) meant that an appreciable proportion of those affected were likely to be vulnerable, and the Appellant had not co-operated fully with the ICO investigation by failing to make full disclosure.

A copy of the case can be found here: **Seaview Brokers Ltd v Information ICO** [EA/2021/0315]

Other recent articles/videos/tools

Global Cookie Review – Second Edition
Consumer Class Actions - Implementation of the new EU Directive tracker
Watch now: Children in the Digital World
The Metaverse
NIS2 Directive – the most important EU cybersecurity act finally adopted
Commission plans initiatives in the domain of virtual worlds, mobility and online piracy
EU institutions discuss and amend new rules on access and use of data
Double-hat DPOs: Berlin Data Protection Authority fines an e-commerce platform for breaching DPO conflict of interest requirements
Data transfers: the US signed an Executive Order to comply with EU law
The German Federal Labour Court refers questions on damages pursuant to Art. 82 GDPR and on the legitimacy of data processing based on a collective agreement to the ECJ
Watch now: How to Create a Child-Safe Platform & Meet Data Privacy Laws
Watch now: The Future of Tech & Data Law

Previous and upcoming events

How to prepare for the Swiss Data Protection Act
Online Safety - a global view: the changing face of regulation for digital businesses
The Metaverse: potential, pitfalls and politics

Recent legal directory rankings

Legal 500 UK - Tier 1, Data Protection, Privacy and Cybersecurity

"The B&B Privacy practice is top notch"
"Great and responsive team with really unique and rare insight into the AdTech market from data privacy perspective."

Chambers UK - Band 1, Data Protection & Information Law

"They are a well-known, large, specialist and dedicated team doing a lot of work with leading tech clients"
"The firm has a strong international network, and its people are really knowledgeable and great to work with."

Ruth Boardman

Partner

+442074156018
ruth.boardman@twobirds.com

Ariane Mole

Partner

+33 (0)1 4268 6000
ariane.mole@twobirds.com

Elizabeth Upton

Legal Director

+442079056280
elizabeth.upton@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority (SRA) with SRA ID497264. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.